

Dkt. 01139

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re Application of:

Boris SUSSMANN

Group Art Unit:

Serial No. (not assigned)

Examiner:

Filed: Concurrently Herewith

For: PROCESS FOR TRANSFER OF DATA INTO
OR OUT OF A CONTROL APPARATUS AS A
MEMORY-PROGRAMMABLE CONTROL UNIT AS
WELL AS CONTROL APPARATUS

PRIORITY DOCUMENT

Honorable Commissioner of Patents and Trademarks

Washington, D. C. 20231

Sir:

Attached is a certified copy of German Application No.
100 38 779.9, filed August 9, 2000, upon which Convention
priority is claimed in connection with the above-identified
application.

It is respectfully requested that receipt of this
priority document be acknowledged.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Scott T. Wakeman".

Scott T. Wakeman
Reg. No. 37,750
(703) 412-1155 Ext. 17

BUNDESREPUBLIK DEUTSCHLAND



11011 U.S. PRO
09/925016
08/09/01

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

Aktenzeichen: 100 38 779.9

Anmeldetag: 09. August 2000

Anmelder/Inhaber: Schneider Automation GmbH,
Seligenstadt/DE

Bezeichnung: Verfahren zur Übertragung von Daten in ein oder
aus einem Steuerungsgerät wie speicher-
programmierbare Steuerung sowie Steuerungsgerät

IPC: G 05 B 19/048

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ur-
sprünglichen Unterlagen dieser Patentanmeldung.

München, den 28. Juni 2001
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Wallner

Schneider Automation GmbH
Steinheimer Str. 117

63500 Seligenstadt

Beschreibung

Verfahren zur Übertragung von Daten in ein oder aus einem Steuerungsgerät wie speicherprogrammierbare Steuerung sowie Steuerungsgerät

Die Erfindung bezieht sich auf ein Verfahren zur Übertragung von Daten in ein oder aus einem Steuerungsgerät sowie auf ein Steuerungsgerät.

Nach dem Stand der Technik werden bei einem Steuerungsgerät Software-Updates wie beispielsweise ein Firmware-Update durch einen Techniker mit einem speziellen Programmiergerät vor Ort durchgeführt. Dabei hat der Techniker nach Eingabe eines entsprechenden Passwortes Zugriff auf den gesamten Speicherbereich, so dass dieser manipuliert werden kann. Oft besteht auch die Notwendigkeit, einem Anwender des Steuerungsgerätes entsprechende Zugriffe beispielsweise zur Änderung und Aktualisierung von Prozessdaten zur Verfügung zu stellen, wobei der Nachteil besteht, dass durch ungeschultes Personal wichtige Programmteile zerstört werden können.

In jüngster Zeit können Steuerungsgeräte wie speicherprogrammierbare Steuerungen auch über Datennetze wie beispielsweise ein Intranet oder das Internet manipuliert bzw. programmiert werden. Dabei tritt ebenfalls das Problem auf, dass nicht autorisierte Personen und/oder nicht autorisierte Programme/Daten Zugriff auf die speicherprogrammierbare Steuerungen erhalten und somit eine ungewollte Zustandsänderung der speicherprogrammierbaren Steuerungen verursachen.

Davon ausgehend liegt der vorliegenden Erfindung das Problem zu Grunde, ein Verfahren und ein Steuerungserät der zuvor genannten Art dahingehend weiterzubilden, dass die Sicherheit der Datenübertragung von und zu dem Steuerungsggerät verbessert wird. Insbesondere sollen nur autorisierte Personen Zugriff auf das Steuerungsggerät erhalten.

Die Lösung des Problems erfolgt durch folgende erfindungsgemäßen Verfahrensschritte:

- Codieren der Daten senderseitig mit zumindest einer individuellen Senderkennung,
- Decodieren der Daten empfängerseitig und Prüfen der individuellen Senderkennung auf Gültigkeit,
- Vergleich der individuellen Senderkennung mit definierten Senderkennungen,
- Zuteilung von Benutzerrechten zur Zustandsänderung der übertragenen Daten und/oder des Steuerungsggerätes entsprechend einer empfängerseitig hinterlegten Berechtigungsliste, sofern die individuelle Senderkennung in der Berechtigungsliste aufgeführt ist,
- Verwerfen der Daten, sofern die individuelle Senderkennung ungültig oder nicht in der Berechtigungsliste aufgeführt ist.

Das erfindungsgemäße Verfahren bietet den Vorteil, dass nur autorisierten Personen mit einer definierten Senderkennung und/oder entsprechend codierten Programmen der Zugriff auf das Steuerungsggerät ermöglicht wird. Dadurch ist gewährleistet, dass eine Änderung von in dem Speicher des Steuerungsggerätes enthaltenen Firmware, Anwendungsprogrammen und Prozessdaten nur von dem Hersteller bzw. den dafür autorisierten Personen durchführbar ist.

Eine bevorzugte Ausführungsform sieht vor, dass die Daten senderseitig mit einer digitalen Signatur und/oder einem öffentlichen Schlüssel (public key) codiert werden und dass die Daten empfängerseitig mit einem zugehörigen geheimen Schlüssel decodiert und/oder die digitale Signatur verifiziert wird. Dies bedeutet, dass jeder Transfer von Daten zu oder von einem Steuerungsggerät wie speicherprogrammierbare Steuerung (SPS) digital unterschrieben ist (digitale Signatur). Nach einem Transfer wird zuerst die Signatur geprüft. Ist diese ungültig, so werden die transferierten Daten verworfen; anderenfalls wird überprüft, ob der Unterschreibende die nötigen Rechte hat, um den Transfer durchzuführen. Sofern der Sender

die Rechte besitzt, werden die Daten verarbeitet, ansonsten werden die transferierten Daten verworfen.

Wenn ein Benutzer Daten digital signiert, fügt er den Daten seine digitale Signatur und gegebenenfalls sein Zertifikat hinzu. Ein Zertifikat besteht, wie im Bereich der digitalen Signaturen üblich, zumindest aus der Kennung und dem öffentlichen Schlüssel des Zertifikatinhabers und der digitalen Signatur des Zertifikatherausgebers über die Inhaberdaten. In dem Steuerungsgerät kann die digitale Signatur zur Überprüfung der Identität und Autorisierung des Senders bzw. des Unterschreibenden verwendet werden und den zugehörigen öffentlichen Schlüssel, um mit verschlüsselten Daten zu antworten, die nur der ursprüngliche Absender mit seinem privaten Schlüssel lesen kann. Auch besteht die Möglichkeit, dass die Daten senderseitig mit dem öffentlichen Schlüssel eines Empfängers und dem Steuerungsgerät codiert werden.

Kann das Steuerungsgerät das Zertifikat nicht direkt verifizieren, so bezieht es über die Zertifikatsinfrastruktur solange Zertifikate, bis eine Kette von Zertifikaten aufgebaut wurde, die von einem verifizierbaren Zertifikat aus lückenlos verifiziert werden kann.

Bei der Datenübertragung von dem Steuerungsgerät zu einem Empfänger ist vorgesehen, dass die Daten in dem Steuerungsgerät mit einer digitalen Signatur codiert werden, so dass eine nachträgliche Manipulation der Daten verhindert wird.

Insbesondere können Übertragungsarten und/oder Grenzbereiche definiert werden, wobei bei einer Datenübertragung aus dem Steuerungsgerät eine Codierung mit digitaler Signatur und/oder öffentlichem und/oder privatem Schlüssel erfolgt.

Vorzugsweise ist die Berechtigungsliste empfängerseitig in einem Speicher des Steuerungsgerätes hinterlegt. Der Speicherbereich selbst ist über die Codierung der zu übertragenen Datei gezielt ansteuerbar. Auch ist die Berechtigungsliste individuell anpassbar.

Zur weiteren Erhöhung der Sicherheit ist vorgesehen, dass für die in dem Steuerungsgerät hinterlegten Berechtigungslisten ebenfalls Zugriffsrechte vergeben werden. Mit anderen Worten kann ein Unbefugter den Schutz durch Manipulation der Berechtigungslisten nicht aushebeln.

Ein Steuerungsgerät wie speicherprogrammierbare Steuerung zeichnet sich dadurch aus, dass dieses eine Empfangseinheit mit einer Decodiereinheit zur Decodierung zumindest einer Senderkennung der empfangenen Daten aufweist, wobei das Steuerungsgerät eine Berechtigungsliste aufweist, in der unterschiedlichen Senderkennungen Rechte zur Zustandsänderung des Steuerungsgerätes zugeteilt sind und wobei der Zustand des Steuerungsgerätes bei gültiger und in der Berechtigungsliste aufgeführter Senderkennung entsprechend der in der Liste vergebenen Rechte veränderbar ist.

Um zu gewährleisten, dass von dem als speicherprogrammierbare Steuerung ausgebildeten Steuerungsgerät gesendete Daten nachträglich nicht manipuliert werden können ist vorgesehen, dass das Steuerungsgerät eine Sendereinheit mit einer Codiereinrichtung zur Codierung von zu sendenden Daten aufweist, wobei in der Codiereinrichtung eine digitale Signatur und/oder ein öffentlicher Schlüssel zur Codierung der Daten enthalten ist.

Der Speicherbereich des Steuerungsgerätes ist in definierbare Bereiche unterteilt, wobei für jeden Speicherbereich in einer Berechtigungsliste für verschiedene Senderkennungen Rechte definierbar sind. Beispielsweise kann der Hersteller Rechte derart vergeben, dass ein Firmware-Speicherbereich nur von der dem Hersteller zugeordneten Senderkennung manipulierbar ist. Dadurch ergibt sich der Vorteil, dass sich die Firmware beispielsweise über das Internet aktualisieren lässt oder in Form einer Datei auslieferbar ist, die ein Kunde der speicherprogrammierbaren Steuerung selbst in diese einspeichert. Da die Signatur der Datei bei einer Manipulation ihre Gültigkeit verliert, kann nur die autorisierte Aktualisierung eingespielt werden.

Der Aufbau der erfindungsgemäßen speicherprogrammierbaren Steuerung bietet weiterhin den Vorteil, dass für Maschinenhersteller (im vorliegenden Fall OEM genannt), die die speicherprogrammierbare Steuerung zur Steuerung einer Produktionseinrichtung verwenden, die Berechtigung für einen von dem OEM verwendeten Programmspeicher derart definierbar ist, dass nur der OEM diesen Bereich beschreiben kann und dass sonst kein Unbefugter diesen Bereich lesen darf. Die Berechtigungsliste kann so eingestellt sein, dass ein Kunde des OEM weitere Programmteile in den nicht geschützten Speicherbereichen einspeichern kann.

Zur weiteren Absicherung der Datenübertragung ist vorgesehen, dass ein verschlüsselter Datentransfer erfolgt. Dadurch lassen sich beispielsweise Prozessdaten aus der speicherprogrammierbaren Steuerung auch über unsichere Medien wie beispielsweise das Internet übertragen. Ein verschlüsselter Datentransfer kann auch von einem OEM verwendet werden, um ein Anwendungsprogramm aus der speicherprogrammierbaren Steuerung auszulesen, ohne dass das Anwendungsprogramm beim Datentransfer von Dritten entschlüsselt werden kann.

Weitere Einzelheiten, Vorteile und Merkmale der Erfindung ergeben sich nicht aus den Ansprüchen, den diesen zu entnehmenden Merkmalen - für sich und/oder in Kombination -, sondern auch aus der nachfolgenden Beschreibung eines der Zeichnung zu entnehmenden Ausführungsbeispiels.

Die einzige Figur zeigt rein schematisch ein Verfahren zur Übertragung einer Datei 10 durch einen Sender wie autorisierte Person 12 über ein Medium 14, das im vorliegenden Beispiel als Datennetz wie Intranet oder Internet ausgebildet ist, zu einem Empfänger 16, der im vorliegenden Ausführungsbeispiel als Steuerungsgerät 16 wie speicherprogrammierbare Steuerung oder PC-basierte Steuerung ausgebildet ist.

Die zu sendende Datei 10 wird zunächst codiert, indem der Datei 10 eine digitale Signatur 18 des Benutzers 12 und ein öffentlicher Schlüssel 20 (public key) zugefügt wird. Die Kombination aus digitaler Signatur 18 und öffentlichem Schlüssel 20 kann auch als Zertifikat bezeichnet werden, das bei Certification Authorities (CA) wie beispielsweise Veri Sign erhältlich ist. Die auf diese Weise signierte bzw. codierte Datei 10' wird über das Medium 14 ver-

schlüsselt übertragen. In der speicherprogrammierbaren Steuerung 16 ist ein Wurzelzertifikat 22 enthalten, umfassend eine digitale Signatur 24 sowie einen geheimen privaten und/oder öffentlichen Schlüssel 20, um die Datei 10' zu decodieren. Ist die Signatur 18 ungültig, so wird die transferierte Datei 10' verworfen. Ist die Signatur 18 gültig, wird überprüft, ob der Benutzer 12 die nötigen Rechte hat, um den Transfer durchzuführen. Hierzu ist in dem Steuerungsgerät 16 eine Berechtigungsliste 28 in Form einer Tabelle abgelegt. Sind diese Rechte vorhanden, kann die Datei 10 verarbeitet werden. Ein Speicherbereich der speicherprogrammierbaren Steuerung 16 ist gemäß Ausführungsbeispiel in definierbare Bereiche (BSS, PS, DS) unterteilt. Für jeden Speicherbereich wie beispielsweise Betriebssystemsspeicher (BSS), Programmspeicher (PS) sowie Datenspeicher (DS) sind in der Tabelle 28 für jede Senderkennung ID1 ... IDn, d. h. jede senderseitige digitale Signatur ID 1, ID 2, ..., IDn Rechte wie beispielsweise Lesen (L) und/oder Schreiben (S) definiert.

In dem hier dargestellten Ausführungsbeispiel sind in der Tabelle 28 insgesamt drei Benutzer ID 1 ... ID 3 sowie drei Speicherbereiche BSS, PS und DS definiert. Einem Hersteller der speicherprogrammierbaren Steuerung 16 ist beispielsweise die Senderkennung ID 1 zugeordnet. Sobald eine Datei 10' mit der Signatur ID 1 erkannt wird, werden die Rechte Lesen und Schreiben für sämtliche Speicherbereiche zugeteilt. Durch die dargestellte Berechtigungstabelle ist es beispielsweise nur dem Hersteller erlaubt, den Firmware-Speicherbereich BSS anzusprechen. Auch kann beispielsweise eine signierte Datei 10' einem Kunden ausgeliefert werden mit der Möglichkeit, dass der Kunde die Datei in die speicherprogrammierbare Steuerung 16 einspielt, ohne auf den Speicher selbst Zugriff zu haben.

Auch besteht die Möglichkeit, dass ein Maschinenhersteller (OEM) für die von ihm verwendeten Programmspeicher die Berechtigung so programmiert, dass nur der OEM den Bereich beschreiben und kein Unbefugter daraus lesen darf, wobei jedoch der Kunde weitere Programmteile in nicht geschützten Programmspeicherbereichen unterbringen kann.

Selbstverständlich besteht auch die Möglichkeit, dass in der speicherprogrammierbaren Steuerung 16 selbst eine Zertifikat-Infrastruktur bestehend aus dem öffentlichen Schlüssel 26 (public key), einem privaten Schlüssel (private key) und einer digitalen Signatur 24 enthalten

ist. Dadurch lassen sich Transferarten bzw. Speicherbereiche definieren, bei denen die speicherprogrammierbare Steuerung die Daten digital unterschreibt, wodurch eine nachträgliche Manipulation der Daten verhindert wird. Selbstverständlich werden auch für die Berechtigungslisten/Tabellen 28 die Rechte zum Zugriff verwendet, so dass kein Unbefugter den Schutz durch Manipulation der Listen aushebeln kann.

Des Weiteren lässt sich mit der Zertifikats-Infrastruktur 18, 20, 22, 24, 26 auch ein verschlüsselter Datentransfer bewerkstelligen, so dass Prozessdaten aus der speicherprogrammierbaren Steuerung auch über Medien, wie beispielsweise das Internet übertragen werden können. Der verschlüsselte Datentransfer kann auch von einem Maschinenhersteller (OEM) verwendet werden, um Anwendungsprogramme aus dem Gerät auszulesen, die Dritten nicht zugänglich werden dürfen.

Schneider Automation GmbH
Steinheimer Str. 117

63500 Seligenstadt

Patentansprüche

Verfahren zur Übertragung von Daten in ein oder aus einem Steuerungsgerät wie speicherprogrammierbare Steuerung sowie Steuerungsgerät

1. Verfahren zur Übertragung von Daten in ein oder aus einem Steuerungsgerät (16) wie speicherprogrammierbare Steuerung, gekennzeichnet durch folgende Verfahrensschritte:
 - Codieren der Daten (10) senderseitig mit zumindest einer individuellen Senderkennung (18, 24),
 - Decodieren der Daten (10) empfängerseitig und Prüfen der individuellen Senderkennung (18, 24) auf Gültigkeit,
 - Vergleich der individuellen Senderkennung (18, 24) mit definierten Senderkennungen (ID 1, ID 2 ... ID n),
 - Zuteilung von Benutzerrechten zur Zustandsänderung der übertragenen Daten (10) und/oder des Steuerungsgerätes entsprechend einer empfängerseitig hinterlegten Berechtigungsliste (28), sofern die individuelle Senderkennung (18, 24) in der Berechtigungsliste (28) enthalten ist und
 - Verwerfen der Daten (10), sofern die individuelle Senderkennung (18) ungültig oder nicht in der Berechtigungsliste (28) enthalten ist.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass die Berechtigungsliste (28) empfängerseitig in einem Speicher des Steuerungsgerätes (16) hinterlegt wird.
3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass ein Speicherbereich (BSS, PS, DS) des als speicherprogrammierbare Steuerung ausgebildeten Steuerungsgerätes (16) über die Codierung der zu übertragenen Datei gezielt ansteuerbar ist.
4. Verfahren nach zumindest einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Berechtigungsliste (28) individuell anpassbar ist, wobei eine Manipulation der Berechtigungsliste (28) nur mit entsprechenden Rechten möglich ist.
5. Verfahren nach zumindest einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass Übertragungsarten und/oder Speicherbereiche (BSS, PS, DS) definiert werden, wobei bei einer Datenübertragung aus dem Datenverarbeitungsgerät (16) eine Codierung mit digitaler Signatur (24) und/oder öffentlichem und/oder privatem Schlüssel (26) erfolgt.
6. Verfahren nach zumindest einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Daten (10) senderseitig mit einer digitalen Signatur (18) und einem öffentlichen Schlüssel (20) (public key) codiert werden und dass die Daten (10) empfängerseitig mit einem zugehörigen geheimen Schlüssel (22) decodiert werden.

7. Verfahren nach zumindest einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Daten (10) verschlüsselt übertragen werden.
8. Verfahren nach zumindest einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
dass die Daten (10) über ein Datennetz (14) wie Intranet oder Internet übertragen werden.
9. Steuerungsgerät wie speicherprogrammierbare Steuerung,
dadurch gekennzeichnet,
dass das Steuerungsgerät (16) eine Empfangseinheit mit einer Decodiereinheit zur Decodierung zumindest einer Senderkennung (18) von empfangenen Daten (10') aufweist, dass das Steuerungsgerät (16) eine Berechtigungsliste (28) aufweist, in der unterschiedlichen Senderkennungen (ID 1 ... ID n) Rechte zur Änderung des Zustandes des Steuerungsgerätes (16) zugeteilt sind und dass der Zustand des Steuerungsgerätes bei gültiger und in der Berechtigungsliste (28) enthaltener Senderkennung (ID 1 ... ID n) entsprechend der in der Berechtigungsliste (22) vergebenen Rechte veränderbar ist.
10. Steuerungsgerät nach Anspruch 9,
dadurch gekennzeichnet,
dass das Steuerungsgerät (16) eine Sendeeinheit mit einer Codiereinrichtung zur Codierung von zu sendenden Daten (10) aufweist, dass in der Codiereinrichtung eine digitale Signatur und/oder ein öffentlicher Schlüssel zur Codierung der Daten enthalten ist.

11. Steuerungsgerät nach Anspruch 9 oder 10,
dadurch gekennzeichnet,
dass der Speicherbereich der speicherprogrammierbaren Steuerung in frei definierbare Bereiche (BSS, PS, DS) unterteilt ist, wobei für jeden Speicherbereich (BSS, PS, DS) in der Berechtigungsliste (28) Rechte für verschiedene Senderkennungen (ID 1, ID 2, IDn) definierbar sind.
12. Steuerungsgerät nach Anspruch bis 11,
dadurch gekennzeichnet,
dass das Steuerungsgerät eine speicherprogrammierbare Steuerung ist.

Schneider Automation GmbH
Steinheimer Str. 117
63500 Seligenstadt

Zusammenfassung

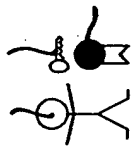
Verfahren zur Übertragung von Daten in ein oder aus einem Steuerungsgerät wie speicherprogrammierbare Steuerung sowie Steuerungsgerät

Die Erfindung bezieht sich auf ein Verfahren zur Übertragung von Daten in ein oder aus einem Steuerungsgerät (16) wie speicherprogrammierbare Steuerung. Zur Erhöhung der Sicherheit der Datenübertragung sind folgende Verfahrensschritte vorgesehen:

- Codieren der Daten (10) senderseitig mit zumindest einer individuellen Senderkennung (18, 24),
- Decodieren der Daten (10) empfängerseitig und Prüfen der individuellen Senderkennung (18, 24) auf Gültigkeit,
- Vergleich der individuellen Senderkennung (18, 24) mit definierten Senderkennungen (ID 1, ID 2 ... ID n),
- Zuteilung von Benutzerrechten zur Zustandsänderung der übertragenen Daten (10) und/oder des Steuerungsgerätes entsprechend einer empfängerseitig hinterlegten Berechtigungsliste (28), sofern die individuelle Senderkennung (18, 24) in der Berechtigungsliste (28) enthalten ist und
- Verwerfen der Daten (10), sofern die individuelle Senderkennung (18) ungültig oder nicht in der Berechtigungsliste (28) enthalten ist.

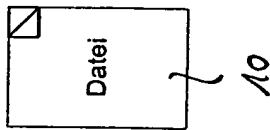
Ein Steuerungsgerät wie speicherprogrammierbare Steuerung zeichnet sich dadurch aus, dass eine Codier- und Decodiereinheit sowie eine Berechtigungsliste vorgesehen sind, in der Benutzerrechte für verschiedene Benutzer hinterlegt sind.

12 20

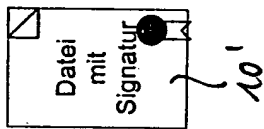


18

Benutzer-ID und
Schlüssel



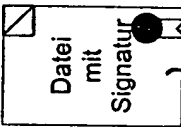
signieren



übertragen

Medium
14

16



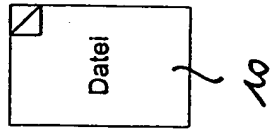
prüfen

28

10 SP	1	2	3
3SS	L+S	X	X
PS	X	L+S	L+S
DS	L+S	L+S	X

Zertifikatsinfra-
struktur und
Rechtelisten

gültig



ungültig

Abbruch

26

24

22